United Nations A/HRC/38/35/Add.5

General Assembly

Distr.: General
13 July 2018

English only

Human Rights Council
Thirty-ninth session
18 June–6 July 2018
Agenda item 3
Promotion and protection of all human rights, civil, political, economic, social and cultural rights, including the right to development

Encryption and Anonymity follow-up report

Note by the Secretariat

The present report by the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression is a follow-up report to the Special Rapporteur's report to the Human Rights Council in 2015 on the use of **encryption and anonymity** to exercise the rights to freedom of opinion and expression in the digital age (A/HRC/29/32). Since 2015, a number of developments have taken place, including a surge in State restrictions on encryption on the one hand, and increased attention to digital security by key sectors of the ICT sector. The Special Rapporteur has followed these trends closely and prepared this report in order to provide an update on the issues identified in the 2015 Report.

GE.18-11662(E)
1811662

Please recycle

I. Introduction

1. In June 2015, the Special Rapporteur's report to the Human Rights Council examined the ways in which encryption protects and promotes freedom of expression. Encryption establishes, among other things, a measure of privacy that enables individuals to search the web, develop opinions and access information online. It may secure the traffic of emails, instant messages and other modes of digital communication so that individuals may express themselves freely. It may protect credit card and banking transactions, business documents, health data, and other sensitive online activities from unauthorized intrusion. The 2015 report also demonstrated how digital security more generally protects art, sexual expression, academic discourse and civil society advocacy in environments of heightened censorship and surveillance.

2. Three years later, however, the challenges users face have increased substantially, while States often see personal, digital security as antithetical to law enforcement, intelligence, and even goals of social or political control. As a result, competing trends and interests have led, on the one hand, to a surge in State restrictions on encryption and, on the other hand, increased attention to digital security by key sectors of the private Information and Communications Technology ("ICT") sector. The Special Rapporteur has followed these trends closely and prepared this report in order to update the Council on the issues identified in the 2015 Report.

3. Part II of this report identifies some of the trends in State restrictions since June 2015 and assesses their compatibility with international human rights law. Part III considers the significant role that corporations play in ensuring respect for freedom of expression, privacy and related human rights through encryption tools. As digital communication has become indispensable to civic engagement and public discourse, companies that enable access to such communication bear important responsibilities to respect the human rights of end users online. This report identifies the responsibilities of these critical actors, building on guidance developed in the Special Rapporteur's 2018, 2017 and 2016 reports to the Human Rights Council.[1]

4. Part IV offers recommendations to States and companies on their duties and responsibilities to safeguard encryption.

II. Trends in State Restrictions on Encryption and Anonymity

A. An Overview of State Obligations

5. The 2015 report demonstrated that a State's obligations to respect and ensure the rights to freedom of opinion and expression and to privacy include the responsibility to protect encryption. Both rights to opinion and expression are well-established under the International Covenant on Civil and Political Rights ("ICCPR"), the Universal Declaration of Human Rights ("UDHR"), regional human rights instruments, and many domestic laws and constitutions.[2] Article 19(1) of the ICCPR establishes the right of everyone to "hold

[1] *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, Human Rights Council, U.N. Doc. A/HRC/38/35 (Apr 6, 2018), *available at* https://documents-dds-ny.un.org/doc/UNDOC/GEN/G18/096/72/PDF/G1809672.pdf?OpenElement; *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, Human Rights Council, U.N. Doc. A/HRC/35/22 (Mar 30, 2017), *available at* https://docs.google.com/viewerng/viewer?url=http://freedex.org/wp-content/blogs.dir/2015/files/2017/05/AHRC3522.pdf&hl=en; *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Human Rights Council*, U.N. Doc. A/HRC/32/38 (May 11, 2016), *available at* https://freedex.org/wp-content/blogs.dir/2015/files/2016/06/A_HRC_32_38_AEV.pdf.

[2] The right to freedom of opinion and expression is established under Articles 19 of the ICCPR and UDHR. The right to privacy is established under Articles 17 and 12 of the ICCPR and UDHR.

opinions without interference". Since the freedom of opinion is absolute, any interference violates the ICCPR.[3] Article 19(2) establishes the right to freedom of expression, defined as the "freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice." The State may only limit the freedom of expression in accordance with the strict requirements of Article 19(3). In particular, restrictions on freedom of expression must be "provided by law" and "necessary" (and proportionate) for the "respect of the rights and reputations of others" and for "the protection of national security or of public order (*ordre public*) or of public health or morals." States have a positive obligation to ensure enabling environments for freedom of expression.[4]

6. Article 17 guarantees the right to be free from "arbitrary or unlawful interference" with one's "privacy, family, home or correspondence," and to the "protection of the law" against such interference. The UN High Commissioner for Human Rights and the Special Rapporteur on freedom of expression have emphasized the close connection between right to privacy and freedom of expression.[5] Encryption secures a "zone of privacy" that enables individuals to develop and share opinions through online correspondence and other digital media.[6] Encryption provides individuals the assurance that their "communications are received only by their intended recipients without interference or alteration, and that the communications they receive are equally free from intrusion."[7] In some cases, encryption may also guarantee anonymity: the use of specially designed encryption schemes such as Tor anonymizes metadata (such as the time, date and place of an individual's communications and online activities) and digital identifiers (such as email or IP addresses).

7. Recognizing the importance of encryption to freedom of expression, privacy and related human rights, the Human Rights Council adopted a resolution in 2017 encouraging "business enterprises to work towards enabling technical solutions to secure and protect the confidentiality of digital communications, which may include measures for encryption and anonymity."[8] The Council also called upon States to refrain from interferences with "the use of such technical solutions" unless they comply with international human rights law.

8. Because of the roles played by encryption, restrictions on their use must satisfy the requirements of legality, necessity and proportionality, and legitimacy. Blanket prohibitions of encryption plainly fail these conditions. Measures that systematically weaken encryption and digital security more generally, such as backdoors, key escrows, and data localization requirements, also interfere with rights to opinion, expression and privacy. Court-ordered decryption should only be permitted on a case-by-case basis applied to individuals pursuant to "transparent and publicly accessible" legal criteria that meet the requirements of Article 19(3) and are subject to prior judicial authorization and associated due process safeguards.[9]

---

[3] Manfred Nowak, *UN Covenant on Civil and Political Rights: CCPR Commentary* (1993), p. 441.

[4] *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye*, Human Rights Council, U.N. Doc. A/HRC/29/32 at ¶ 18 (May 22, 2015), *available at* https://freedex.org/wp-content/blogs.dir/2015/files/2015/10/Dkaye_encryption_annual_report.pdf.

[5] *The right to privacy in the digital age: Report of the United Nations High Commissioner for Human Rights*, Human Rights Council, U.N. Doc. A/HRC/27/37 at ¶ 14, (June 30, 2014), *available at* https://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf; A/HRC/29/32 n. 4 at ¶ 16.

[6] A/HRC/29/32, *id.* at ¶ 16.

[7] *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue*, Human Rights Council, U.N. Doc. A/HRC/23/40 at ¶ 23 (Apr. 17, 2013, *available at* https://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf.

[8] Human Rights Council, U.N. Doc. A/HRC/RES/34/7 at ¶ 9 (Apr 7, 2017).

[9] A/HRC/29/32, supra n. 4, at ¶ 60.

B. State practice: examples and concerns

9. The 2015 Report noted ways in which States interfere – or were then proposing to interfere – with encryption. Since then, State practice has not improved and may have become less protective of digital security. This section examines restrictions on encryption that are inconsistent with the requirements of legality, necessity and proportionality, and legitimacy.

10. There are notable exceptions to the trends described below. The Netherlands, for example, publicly recognizes the benefits of encryption and has not enacted legislation that would guarantee government access to encrypted data.[10] It remains to be seen whether other European Union ("EU") member States will follow suit. Article 25 of the General Data Protection Regulation ("GDPR") establishes data protection "by design and by default," requiring data controllers to implement "appropriate technical and organisational measures" to protect the privacy and other fundamental rights of EU data subjects.[11] The European Data Protection Supervisor has urged member States to adapt or create legal frameworks at the domestic and regional levels that support privacy by default, including the use of privacy enhancing technologies such as end-to-end encryption.[12]

1. Bans on Use and Dissemination of Encryption Tools

11. Many States have adopted criminal laws banning the use and dissemination of encryption technologies. In Pakistan, the 2016 Prevention of Electronic Crimes Act established vague criminal prohibitions on the supply of computer software and the programming of computer systems, which could be broadly interpreted to crack down on the use of encryption tools and networks that provide anonymity (such as Tor and VPNs).[13] Similarly, Iran bans encryption through its Computer Crimes Act.[14] Turkey has arrested and detained thousands of citizens for the alleged use of an encrypted messaging app that the government linked to political opponents it alleges bear responsibility for the July 2016 coup attempt.[15]

2. Licensing and Registration Requirements

12. Laws requiring registration and government approval of encryption tools reverse the well-established presumption that States bear the burden of justifying restrictions on these rights. Vietnam's 2015 Law on Network Information Security requires companies "trading in civil encryption products" to obtain business licenses to do so.[16] In Malawi, the 2016 Electronic Transactions and Cyber Security Act prohibits the provision of cryptography services or products without registration and requires anyone who provides encryption services to disclose key information about the technical aspects of the encryption used to the Malawi Communications Regulatory Authority; violation of these provisions can result

---

[10] ENISA, 'The Netherlands: Cabinet Launched Position on Encryption', ENISA, 21 April 2016; Dutch Ministry of Security and Justice, Cabinet's View on Encryption, 2016.

[11] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, *available at* https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32016R0679 ("General Data Protection Regulation").

[12] European Data Protection Supervisor, Preliminary Opinion on privacy by design (Opinion 5/2018), *available at* https://edps.europa.eu/sites/edp/files/publication/18-05-31_preliminary_opinion_on_privacy_by_design_en_0.pdf.

[13] *See, e.g.*, Special Rapporteur on Promotion and Protection of the Right to Freedom of Expression and Opinion, *Comme'n to Pakistan Regarding Laws on Cyber-Terrorism* (Dec. 14, 2015), *available at* https://spdb.ohchr.org/hrdb/32nd/public_-_OL_Pakistan_14.12.15_(13.2015).pdf.

[14] *See* Computer Crimes Act, Jan. 23, 2010, *available at* https://www.unodc.org/res/cld/document/computer-crimes-act_html/Computer_Crimes_Act.pdf.

[15] A/HRC/35/22, *supra* n. 1 at ¶ 54; Human Rights Council, Working Group on Arbitrary Detention, Opinion No. 38/2017 concerning Kursat Çevik (Turkey), U.N. Doc. A/HRC/WGAD/2017/38 (June 16, 2017) at ¶ 40.

[16] *See* Law on Network Information Security, Art. 31 (July 1, 2016), *available at* http://english.mic.gov.vn/Upload/VanBan/Law-on-Network-Information-Security-16-05-30.pdf.

in large fines and up to seven years of imprisonment. [17] In 2016, Russia adopted the "Yarovaya Law" (Federal Law No. 375-FZ), which also requires authorities to certify the use of encryption technology[18] and establishes administrative penalties for the use of non-certified encryption equipment.[19] Such requirements raise the prospect of direct interference with the ability to use encryption tools without enabling government intrusions through backdoors or other vulnerabilities.

3. Intentional Weakening of Encryption

13. Since 2015, States have intensified their efforts to weaken encryption used in widely available communications products and services. In particular, State pressure on companies to install encryption "backdoors" - security vulnerabilities designed for law enforcement to access encrypted communications or open secured devices - has been mounting. However, there is widespread consensus among information security experts that such vulnerabilities impose significant costs on digital security overall, as they may be exploitable by unauthorized third parties even if they are intended solely for government access.[20] Despite this threat to the privacy and security of *all* users, States have failed to demonstrate the necessity of backdoors, particularly given the wide range of investigative tools at their disposal.

14. The United Kingdom's 2016 Investigatory Powers Act, aimed to place government practices on legal footing, may provide authority for the Government to weaken encryption. The Act provides authorities the power to issue a "technical capability notice" to operators of communications services, including social media platforms, webmail hosts, and cloud services providers.[21] This vaguely formulated authority raises the possibility that operators could be compelled to build backdoors in their networks and also remove end-to-end encryption and cooperate with a wide range of government hacking measures.[22] Other States have looked towards the Act as a model for granting law enforcement and intelligence authorities wide latitude to access encrypted data and conduct intrusive surveillance. In 2017, for example, Australia announced its intention to introduce cybersecurity legislation that would "impose an obligation upon device manufacturers and … service providers to provide appropriate assistance to intelligence and law enforcement on a warranted basis."[23] Similarly, China's 2016 Cybersecurity Law requires network operators to "provide technical support and assistance" to state and public security organs for the purposes of national security and law enforcement.[24]

15. Elsewhere, the battle to protect encryption in commercially available products and services has escalated to the courts, with mixed results. Following a 2015 attack in San Bernardino, California, that left 14 people dead, the U.S. Federal Bureau of Investigation ("FBI") sought to compel Apple to create software that would disable security features on the suspect's iPhone. The FBI ultimately withdrew its request when it secured access to the cell phone data with the assistance of an unidentified third party. However, the dispute highlighted how security vulnerabilities introduced on a single device and for a specific

---

[17] Electronic Transactions and Cyber Security Act, ss. 52, 53 (Oct. 20, 2016), *available at* https://www.malawilii.org/mw/legislation/act/2016/33.

[18] *Overview of the Package of Changes into a Number of Laws of the Russian Federation Designed to Provide for Additional Measures to Counteract Terrorism*, The International Center for Not-for-Profit Law, *available at* http://www.icnl.org/research/library/files/Russia/Yarovaya.pdf.

[19] *Id.*

[20] *See Decrypting the Encryption Debate: A Framework for Decision Makers*, The National Academies Press, https://www.nap.edu/read/25010/chapter/6.

[21] *See* Investigatory Powers Act, s. 253 (Nov. 29, 2016), *available at* https://www.legislation.gov.uk/ukpga/2016/25/section/253.

[22] *See Joint Commc'n to United Kingdom Regarding Law on Expansive Government Powers* (Aug. 19, 2015), hhttps://spdb.ohchr.org/hrdb/32nd/public_-_OL_United_Kingdom_22.12.15_%284.2015%29.pdf

[23] *See* Prime Minister, National Security Statement (Jun 13, 2017), *available at* https://www.pm.gov.au/media/national-security-statement.

[24] *See* Cybersecurity Law, Art. 28 (Nov. 7, 2016), available at https://www.chinalawtranslate.com/cybersecuritylaw/?lang=en.

investigation could nevertheless be exploited to compromise all devices of the same model or type.[25] At the request of the government, a district court in the Russian Federation issued a ruling blocking access to Telegram, a popular messaging app, after the company refused to provide encryption keys to the government as may be required under the "Yarovaya Law."[26] This ruling follows a Constitutional Court decision that effectively eliminates the need for a judicial warrant to review and analyze information stored on electronic devices "seized during the course of investigative activities."[27] Soon after Russia's moves, Iran issued its own ban on the use of Telegram, a widely used tool for communication in the country.[28]

4. Government Hacking

16. A growing number of States has also seized on the prevalence of encrypted communications as justification for broad and intrusive government hacking regimes. Hacking is difficult to define, given the broad scope of activities it covers. A leading digital rights organization understands hacking to be "the manipulation of software, data, a computer system network or other electronic device" without the permission or knowledge of their owners, custodians or users;[29] another defines it more broadly to include any interference with a system that "caus[es] it to act in a manner unintended or unforeseen by the manufacturer, user or owner of that system."[30] In addition to compromising encryption, governments have employed hacking to conduct surveillance, manipulate data, and launch Denial of Service attacks to force the shutdown of particular websites or services, among other uses.[31]

17. Civil society organizations have documented and exposed government hacking activities around the world. Uganda's military intelligence and law enforcement agencies reportedly employed Finfisher, a commercial malware tool, to collect information about "negative minded politicians" with the aim of "easily crushing them by being a step ahead."[32] In Mexico, multiple reports indicate that government authorities are using malware to track and monitor broad swaths of civil society, including journalists, lawyers, anti-corruption activists, food scientists and health and consumer advocates.[33] Encryption provides little or no protection against these advanced hacking tools, which typically trick targets into installing them on their devices and providing unfettered third party access to their data.

---

[25] *See Letter to U.S. Judge Regarding Seizure of Mobile Phone and Search Warrant* (March 2, 2016), https://freedex.org/wp-content/blogs.dir/2015/files/2017/08/Letter_from_David_Kaye_UN_Special_Rapporteur_on_the_promotion_and_protection_of_the_right_to_freedom_of_opinion_and_expression.pdf.

[26] *See Joint Commc'n to Russia Regarding Amendments to Criminal Code* (July 28, 2016), http://www.ohchr.org/Documents/Issues/Opinion/Legislation/RUS_7_2016.pdf.

[27] Peter Roudik, *Russia: No Warrant Needed for Chat and Email Eavesdropping* (Mar. 29, 2018), available at http://www.loc.gov/law/foreign-news/article/russia-no-warrant-needed-for-chat-and-email-eavesdropping/

[28] Human Rights Watch, *Iran: Assault on Access to Information* (May 2, 2018), *available at* https://www.hrw.org/news/2018/05/02/iran-assault-access-information.

[29] Access Now, *A Human Rights Response to Government Hacking* (September 2016), *available at* https://www.accessnow.org/cms/assets/uploads/2016/09/GovernmentHackingDoc.pdf.

[30] Privacy International, Hacking Safeguards and Legal Commentary (Jun 11, 2018), *available at* https://privacyinternational.org/advocacy-briefing/1057/hacking-safeguards-and-legal-commentary.

[31] *Id.*

[32] Brief for Privacy International as Amicus Curiae, U.S. v. Werdene, 883 F.3d 204 (2018), *available at* https://privacyinternational.org/sites/default/files/2017-11/2017-04-26-US-v-Werdene-Amicus-BriefECF.pdf ("PI Werdene brief").

[33] Bill Marczak and John Scott-Railton, *Reckless Exploit: Mexican Journalists, Lawyers, and a Child Targeted with NSO Spyware* (Jun 19, 2017), *available at* https://citizenlab.ca/2017/06/reckless-exploit-mexico-nso/; John Scott-Railton, Bill Marczak, Claudio Guarnieri, and Masashi Crete-Nishihata, *Bittersweet: Supporters of Mexico's Soda Tax Targeted With NSO Exploit* (Feb 11, 2017), *available at* https://citizenlab.ca/2017/02/bittersweet-nso-mexico-spyware/.

18. Even where government hacking is authorized by law, relevant legal frameworks are typically crafted in vague and ambiguous language, providing the authorities open-ended powers with minimal external oversight. In the United Kingdom, the intelligence agency GCHQ reportedly has been obtaining general warrants to conduct large-scale hacking under Section 5 of the Intelligence Services Act 1994, which permits the Secretary of State to issue such warrants authorizing government interference with "property or with wireless telegraphy."[34] At the time of publication of the present report, civil society organizations are challenging GCHQ's authority before the UK Supreme Court and the European Court of Human Rights.[35] In Italy, human rights groups have criticized a Bill to regulate the government's use of hacking tools, arguing that it provides broad carve-outs for intelligence agencies, does not cover many hacking activities, and fails to specify the considerations of necessity and proportionality that judges should take into account when issuing a hacking warrant.[36] In the United States, a 2016 amendment to Federal Rule of Criminal Procedure 41 permits judges to issue warrants authorizing law enforcement "to use remote access to search electronic storage media" anywhere in the country and around the world.[37] In 2015, the U.S. Federal Bureau of Investigations reportedly obtained a warrant under Rule 41 to hack more than 8,700 devices in 120 countries and territories.[38]

5. Mandatory Data Localization and Key Escrows

19. Government authorities increasingly require providers of communications services operating in their jurisdiction to store personal and sensitive data locally, including encryption keys that secure such data. In February 2018, Apple announced plans to store encryption keys for Chinese iCloud accounts within China, in order to comply with data localization requirements under the 2016 Cybersecurity Law.[39] Local storage of encryption keys may also be required in Russia (under its Yarovaya Law) and Kazakhstan, which mandate the storage of any personal data collected from its citizens within the country.[40] Data localization mandates raise concern that easy government access to locally stored encryption keys and other sensitive data will be abused to surveil and stifle expression and dissent.

20. Mandatory key escrows go even further, requiring communications service providers to store encryption keys with a designated government authority or a 'trusted third party.' In the United States, the Department of Justice reportedly sought to compel

---

[34] *Privacy International and Others v. United Kingdom*, [2016] UKIP Trib 14_85-CH, *available at* https://privacyinternational.org/sites/default/files/2018-03/2016.02.12%20Hacking%20Judgment.pdf.

[35] Privacy International, *The Queen on the application of Privacy International v. Investigatory Powers Tribunal (UK General Hacking Warrants)*, Case No. UKSC 2018/0004 (Supreme Court) / C1/2017/0470/A (Court of Appeal) / CO/2368/2016 (High Court), *available at* https://privacyinternational.org/legal-action/queen-application-privacy-international-v-investigatory-powers-tribunal-uk-general; *Big Brother Watch and Others v. the United Kingdom* (European Court of Human Rights, no. 58170/13), *Bureau of Investigative Journalism and Alice Ross v. the United Kingdom* (ECtHR no. 62322/14) and *10 Human Rights Organisations and Others v. the United Kingdom* (ECtHR no. 24960/15).

[36] Privacy International, *Privacy International's Analysis of the Italian Hacking Reform, under DDL Orlando* (Mar 5, 2017), *available at* https://privacyinternational.org/sites/default/files/2018-01/PI_hacking_DDL%20Orlando.pdf; Access Now, *Re: Disciplina dell'uso dei captatori legali nel rispetto delle garanzie individuali* (Mar 29, 2017), *available at* https://www.accessnow.org/cms/assets/uploads/2017/05/Access-Now-Comment-Disciplina-dell%E2%80%99uso-dei-captatori-legali.pdf.

[37] Fed. R. Crim. P. 41.

[38] PI Werdene Brief, *supra* n. 32.

[39] Human Rights Watch, *World Report 2018*, available at https://www.hrw.org/world-report/2018/country-chapters/china-and-tibet.

[40] On Amendments to Certain Legislative Acts of the Republic of Kazakhstan on Informatization' (24 November 2015 No. 419-V); *see also* 'Bret Cohen, Britanie Hall, and Charlie Wood, Data Localization Laws And Their Impact On Privacy, Data Security And the Global Economy, *Antitrust*, Vol. 32 No. 1, Fall 2017, 111, at https://www.americanbar.org/content/dam/aba/publications/antitrust_magazine/anti_fall2017_cohen.authcheckdam.pdf.

software companies to hand over their source code and private encryption keys to government authorities under gag order.[41] As the 2015 Report emphasized, key escrows increase the risks of hacking, attacks and other forms of misuse that undermine users' security and privacy.[42]

6. Restrictions on Encryption Tools Designed to Protect Anonymity

21. Certain encryption tools and features are designed not only to protect the content of communications, but also information about the identity, contact details and whereabouts of users exchanging or accessing information online. For example, a Virtual Private Network ("VPN") can route Internet traffic through virtual encrypted tunnels, protecting the identity of users and providing a gateway to access geo-blocked and censored websites. Given that digital anonymity has become indispensable to the exercise of privacy and freedom of expression, restrictions on digital anonymity must also satisfy the requirements of legality, necessity and proportionality, and legitimacy.[43]

22. Despite these requirements, some States have imposed undue restrictions on the right to anonymity online. In South Korea, for example, law enforcement is permitted to access customer identity data held by telecommunications providers without a warrant; a group of digital rights advocates has challenged this legal authority before the Constitutional Court of Korea.[44] The 2015 report also noted the problems raised by SIM card registration.[45] In 2017, Germany tightened security laws relating to the registration of users at the time of purchasing a SIM card.[46] In Russia, providers of communications services have been forced to disclose the identity of users under government investigation.[47] In China, Apple bowed to government pressure to remove VPN services from its China App Store after a law was passed to restrict the use of VPNs on the State network infrastructure.[48]

III. The Role of Corporations

23. The 2015 Report explained that "[e]ncryption and anonymity may be promoted or compromised" by a range of corporate actors, including telecommunications and Internet service providers ("Telcos and ISPs"), messaging and social media platforms, search engines and cloud services.[49] Although companies are not parties to the Covenant, they nevertheless significantly impact privacy and freedom of expression. The United Nations Guiding Principles on Business and Human Rights establish that business enterprises should, at a minimum, make *high-level policy commitments* to human rights; conduct *due diligence* and take other appropriate action that identifies, prevents, mitigates, and accounts for human rights impacts associated with their activities; and provide appropriate *remediation* for abuses that occur as a result of company practices.[50] The Special

---

[41] Bruce Schneier, *Companies Handing Source Code Over to Governments* (Mar 18, 2016), *available at* https://www.schneier.com/blog/archives/2016/03/companies_handi.html.

[42] A/HRC/29/32, supra n. 4 at ¶ 44.

[43] A/HRC/29/32, supra n. 4, at ¶ 47.

[44] *See Intervention Submission to Korean Court Regarding Law Enforcement and Anonymity*, available at https://freedex.org/wp-content/blogs.dir/2015/files/2017/05/2016Heonma388-English.pdf.

[45] A/HRC/29/32, supra n. 4, at ¶ 51.

[46] Anna Biselli, *Interaktive Karte: Registrierungspflicht für Prepaid-SIM-Karten in Europa weit verbreitet*, Netzpolitik.org (Aug 2, 2017), *available at* https://netzpolitik.org/2017/interaktive-karte-registrierungspflicht-fuer-prepaid-sim-karten-in-europa-weit-verbreitet.

[47] *Freedom on the Net 2017*, Freedom House, available at https://freedomhouse.org/report/freedom-net/2017/russia.

[48] *See Comm'n to Apple CEO Regarding Removal of VPN Applications* (Aug. 14, 2017), http://www.ohchr.org/Documents/Issues/Opinion/Legislation/OLOTH.pdf.

[49] A/HRC/29/32, supra n. 4, at ¶ 28.

[50] United Nations, *Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect, and Remedy Framework* (2011), at Principle 15, available at http://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf

Rapporteur has synthesized these principles into issue-specific guidance for Internet companies and digital access providers.[51] These principles have also framed multi-stakeholder, inter-governmental and civil society discourse concerning the human rights responsibilities of the ICT sector.[52]

24. Messaging apps, device manufacturers and digital access providers in particular play vital roles in facilitating privacy and freedom of expression. Giving the burgeoning popularity of messaging apps, companies providing this service handle a massive volume of sensitive and personal communications that are vulnerable to government or third-party interference unless secured by encryption and other protective measures. It has also become industry practice for manufacturers of computers, laptops, mobile phones and other Internet-connected devices to equip them with built-in encryption tools that secure the data stored on or transmitted by them. Digital access providers, which provide critical communications infrastructure, bear a responsibility to refrain from undue interference with encrypted communications and the anonymity of end users. This section discusses the extent to which popular messaging apps, device manufacturers and major digital access providers have satisfied these responsibilities, and the challenges they continue to face. Although this section does not exhaustively document the roles of the ICT sector in facilitating encryption, the principles here apply to all private companies providing security to their users.

A. Messaging Apps

25. Messaging apps enable an ever-broadening range of digital communications between users, including instant messaging, photo, video and file sharing, and voice and video calls. In recent years, messaging apps have also been developed into broad, multifaceted platforms that enable mobile payments, e-commerce, gaming, and status updates. For example, WeChat[53], the most popular messaging app in China with over 900 million active users at the time of publication, has been described as an "online ecosystem where people can shop, browse news, book gym classes, plan events, and order taxis."[54] Other messaging apps, such as WhatsApp[55], Viber[56] and Telegram[57], have also become the backbone of digital life for tens of millions of individuals, providing a popular means of communication and access to information.

---

[51] A/HRC/38/35, *supra* n. 1; A/HRC/35/22, *supra* n. 1.

[52] See Global Network Initiative, *Principles on Freedom of Expression and Privacy* (last updated May 2017), available at https://globalnetworkinitiative.org/gni_tnetnoc/uploads/2018/04/GNI-Principles-on-Freedom-of-Expression-and-Privacy.pdf; European Commission, *ICT Sector Guide on Implementing the UN Guiding Principles on Business and Human Right*, available at https://www.ihrb.org/pdf/eu-sector-guidance/EC-Guides/ICT/EC-Guide_ICT.pdf.

[53] WeChat is a social media and messaging platform owned by Chinese company, Tencent.

[54] Pen America, *FORBIDDEN FEEDS: Government Controls on Social Media in China*, p.12, available at https://pen.org/wp-content/uploads/2018/03/PENAmerica_Forbidden-Feeds-3.13-3.pdf (March 13, 2018)

[55] WhatsApp, which was purchased by Facebook in 2014, allows users to send text messages, as well as voice and video calls.

[56] Viber is a text, audio, and video messaging application owned by Japanese multinational company Rakuten.

[57] Telegram is cloud-based messaging platform launched in 2013 by the founders of the Russian social network VK.

A closer look at Signal, a non-profit messaging app

Signal is a secure mobile and desktop messaging application that enables users to exchange end-to-end encrypted text, audio, and video messages. Signal was initially released by Open Whisper Systems in July 2014, and was founded on the principle "that private communication could be simple."[58] Unlike the other platforms reviewed in this report, Signal is able to focus on security and privacy without market-based pressures. Although Open Whisper Systems is not a registered non-profit, the organization is primarily funded through grants and donations and therefore does not rely on advertisement revenue or subscriber fees. [59] Moreover, in February 2018, Open Whisper Systems announced the creation of Signal Foundation, a registered non-profit funded by a $50,000,000 donation from WhatsApp co-founder, Brian Acton, who now heads the organization.[60] Signal Foundation's core purpose is to "support, accelerate, and broaden Signal's mission of making private communication accessible and ubiquitous."[61] Like WhatsApp and Facebook Messenger, Signal relies on Open Whisper Systems open source Signal Protocol. Unlike Facebook Messenger, however, all Signal messages are encrypted by default. Signal also recognizes the need for outside professionals to conduct regular security audits on their encryption protocols, with publicly available results. To this end, it provides "the complete source code for the Signal clients and the Signal server" on GitHub.[62]

Although Signal is highly regarded in the secure communications space, it is not without flaws. Open Whisper Systems's founder claims the platform does not store any user metadata, though he has acknowledged the platform stores information detailing the last day a user accessed Signal's server. [63] Signal's brief privacy policy states the platform only temporarily stores the information necessary to function, like IP addresses and information "transmitted to the server in order to determine which of your contacts are registered."[64] However, critics have raised concerns about Signal's reliability[65] and the fact that Signal's relatively smaller user-base may create greater suspicion for individuals hoping to engage in secure communications than more mainstream applications like iMessage, WhatsApp, or Facebook Messenger.[66] Indeed, although Signal leads the way with respect to its' technical capabilities and minimal data collection, whether or not Signal should be hailed as the standard for secure communications requires a consideration of individual user needs.

26. *High-Level Policy Commitments:* Recognizing their importance to digital communication and in keeping with the UN Guiding Principles, most messaging apps have issued policy statements specifying their commitment to the privacy of their users. Viber, a Japanese messaging app, states that the company's mission is to "protect . . . privacy so that you never have to think twice about what you can or can't share when you're using Viber."[67] Telegram specifically embraces a commitment to protecting private conversations and personal data from "third parties" such as officials, employers, markets and

[58] Signal, *Signal Foundation* (February 21, 2018), available at https://signal.org/blog/signal-foundation/

[59] Signal, *How Can I Donate*, available at https://support.signal.org/hc/en-us/articles/212940158-How-can-I-donate-

[60] Signal, *Signal Foundation*, supra. n. 58.

[61] Id.

[62] See Signal, *Is it private? Can I trust it?*, available at https://support.signal.org/hc/en-us/articles/212477768-Is-it-private-Can-I-trust-it-

[63] Micah Lee, *BATTLE OF THE SECURE MESSAGING APPS: HOW SIGNAL BEATS WHATSAPP*, The Intercept (June 22, 2016) available at https://theintercept.com/2016/06/22/battle-of-the-secure-messaging-apps-how-signal-beats-whatsapp/

[64] Signal, *Privacy Policy*, available at https://signal.org/signal/privacy/

[65] Taylor Hatmaker, *Encrypted chat app Signal goes down for some users*, TechCrunch (Oct. 17, 2017), available at https://techcrunch.com/2017/10/27/is-signal-down/

[66] Gen.ac Gebhart, *Why We Can't Give You a Recommendation*, Electronic Frontier Foundation (March 27, 2018) available at https://www.eff.org/deeplinks/2018/03/why-we-cant-give-you-recommendation

[67] Rakuten Viber, *Security*, available at https://www.viber.com/security/

advertisers.[68] Although WeChat claims that "user privacy and data protection are [their] top priorities," it commits only to encrypting "sent and received messages between [its] servers and [the user's] device" to prevent third party interference as they are being delivered over the Internet.[69]

27. *The Responsibility to Provide Encryption*: Whether or not messaging apps fulfil their human rights obligations depends on how they design, maintain and educate users about privacy and security safeguards on their platforms. The UN Guiding Principles indicate that companies should undertake due diligence and other appropriate action to prevent, mitigate and account for adverse human rights impacts connected to their business activities. In the context of messaging, unsecured communications are likely to expose users to a broad range of privacy and freedom of expression interferences, including data breaches, hacking, identity theft and undue government surveillance. Accordingly, the responsibility to prevent or mitigate these impacts requires messaging apps to assess "the role that tools such as encryption, anonymizing technologies, security enhancements and proxy technologies can play in enabling users to manage their media experiences and protect freedom of expression and privacy."[70] These assessments often require intricate and ongoing analysis of the trade-offs between security, costs of implementation, ease of use, message delivery and service availability.[71]

28. End-to-end encryption has become "the most basic building block" for digital security on messaging apps, and several apps offer this layer of security as a matter of default.[72] WhatsApp adopted end-to-end encryption for all messages by default in April 2016, however, recent reporting has raised concern that Facebook may soon take measures to weaken the platform's encryption capabilities.[73] LINE also introduced end-to-end encryption in July 2016;[74] Apple's iMessage service has been end-to-end encrypted since 2011.[75] Viber began offering end-to-end encryption for its users in both one-on-one and group chats in 2016, provided users were using the most updated version of the

---

[68] Telegram, *Telegram FAQ*, available at https://telegram.org/faq#q-what-are-your-thoughts-on-internet-privacy

[69] WeChat Help Center, *How secure are my chat messages and conversations on WeChat? Can third-parties snoop or read my messages?*, available at https://help.wechat.com/cgi-bin/micromsgbin/oshelpcenter?opcode=2&plat=1&lang=en&id=1208117b2mai1410243yyQFZ&Channel=helpcenter

[70] Global Network Initiative, *IMPLEMENTATION GUIDELINES FOR THE PRINCIPLES ON FREEDOM OF EXPRESSION AND PRIVACY*, s. 4.9, available at https://globalnetworkinitiative.org/wp-content/uploads/2017/07/Implementation-Guidelines-for-the-GNI-Principles.pdf

[71] Erica Portnoy, *Building a Secure Messenger*, Electronic Frontier Foundation (March 29, 2018), available at https://www.eff.org/deeplinks/2018/03/building-secure-messenger

[72] *Ibid.*

[73] See WhatsApp, *Legal Info*, available at https://www.whatsapp.com/legal?eea=1#key-updates; see also Aatif Sulley, *WhatsApp Encryption: What Is It, How Does It Work, and Why Is the Government So Worried About It?* Independent (March 27, 2017), available at https://www.independent.co.uk/life-style/gadgets-and-tech/features/whatsapp-encryption-what-is-it-how-does-it-work-why-ban-it-backdoor-access-secret-messages-a7652396.html; but see Chris Smith, *Jan Koum is leaving Facebook and WhatsApp users will end up paying the price*, BGR (May 1, 2018), available at http://bgr.com/2018/05/01/whatsapp-founder-jan-koum-leaving-facebook-encryption-doomed/

[74] See LINE, *Encryption Report* (March 24, 2016), available at https://linecorp.com/en/security/encryption_report; see also Paul Sewers, *Ahead of IPO, mobile messaging giant Line introduces end-to-end encryption by default*, Venture Beat (June 30, 2016), available at https://venturebeat.com/2016/06/30/ahead-of-ipo-mobile-messaging-giant-line-introduces-end-to-end-encryption-by-default/. LINE is a Japanese platform that allows users (individually or within groups) to communicate via text messaging, audio calls, video conferencing, and gaming.

[75] See Apple, *Apple Privacy*, available at https://www.apple.com/privacy/approach-to-privacy/; see also Sam Brindle, *Apple Logs Your iMessage Contacts – And May Share Them With the Police*, the Intercept (September 28, 2016), available at https://theintercept.com/2016/09/28/apple-logs-your-imessage-contacts-and-may-share-them-with-police/

application.[76] Despite the growing adoption of end-to-end encryption, however, the scope of metadata retained about communications sent and received on these apps, and how such metadata is used or shared, is unclear.[77]

29. In contrast, other companies do not enable end-to-end encryption by default and leave users the option of enabling this functionality based on individual assessment of security and messaging needs. Facebook, for example, requires users to "opt-in" to end-to-end encrypted conversations on the Facebook Messenger[78] app on iOS and Android; notably, this functionality cannot be enabled on web-based services such as facebook.com and messenger.com.[79] Telegram users are protected by end-to-end encryption only if they enable "Secret Chats:" Unlike the app's regular "Cloud Chats," these messages are not backed up on the company's private cloud, cannot be forwarded and can be set to self-destruct.[80] Deletion of messages on one side of a "Secret Chat" will also lead to deletion on the other side of the communication.[81]

30. In general, the responsibility to safeguard freedom of expression and privacy may require companies to establish end-to-end encryption as a default setting in their messaging products. When companies do not provide this feature by default, they should ensure that the "opt-in" feature is highly visible and user-friendly and provide clear and accessible information regarding the differences between various privacy settings.[82]

31. *Policy Safeguards*: Beyond technical security measures, the responsibility to respect user privacy also encompasses the development and implementation of policy safeguards that prevent or mitigate undue government and private interference. For example, the failure to develop a strategy for preventing or mitigating government demands for mandatory key escrows and other decryption measures will offset the benefits of providing end-to-end encryption. More broadly, clear and accessible policies on data collection, handling, sharing and retention, such as law enforcement guidelines and advertising policies, are also essential. For example, Telegram explains that, since it stores user data in multiple jurisdictions, a request for such information would be required to "pass the scrutiny of several different legal systems around the world."[83] WhatsApp requires law enforcement to submit requests for records "with particularity" that include, at a minimum, the name of the issuing authority, proof of identity, a direct contact phone number, and the

---

[76] Generally, all one-to-one messages will be encrypted if both users have Version 6.0 of the application or newer. Similarly, group chats will also be encrypted provided each member of the group is using a recent version of Viber. However, the support website states that "the more public groups such as Public Chats and Communities are not end-to-end encrypted." In order to determine whether or not a particular conversation is actually encrypted, Viber instructs users to check the "chat info screen" for the following message that states "Messages sent by the participants in this conversation are encrypted. See Rakuten Viber Support, *VIBER'S ACCOUNTS SECURITY AND ENCRYPTION*, available at https://support.viber.com/customer/en/portal/articles/2017401-viber-accounts-security-and-encryption#group-charts; see also Kate Conger, *Viber Defends New End-to-End Encryption Protocol Against Criticism, TechCrunch* (April 20, 2016), available at https://tech.runch.com/2016/04/20/viber-defends-new-end-to-end-encryption-protocol-against-criticism/

[77] For example, Apple maintains "capability query logs" regarding the use of iMessage and other applications, however, it is difficult to determine precisely how much information these logs may retain. See Sam Brindle, *Apple Logs Your iMessage Contacts: And May Share Them With the Police*, the Intercept, 28 September 2016, available at https://theintercept.com/2016/09/28/apple-logs-your-imessage-contacts-and-may-share-them-with-police/

[78] Facebook Messenger is one of the most widely used text, audio, and video messaging applications with over 1.2 billion users.

[79] Facebook, *Secret Conversations*, available at https://www.facebook.com/help/messenger-app/1084673321594605/?helpref=hc_fnav

[80] Telegram, *FAQ For the Technically Inclined*, available at https://core.telegram.org/techfaq#q-how-does-end-to-end-encryption-work-in-mtproto

[81] *Ibid.*

[82] See *infra* text accompanying n. 87 – 90.

[83] Pavel Durov, *Why Isn't Telegram End-to-End Encrypted by Default?* (August 14, 2017), available at http://telegra.ph/Why-Isnt-Telegram-End-to-End-Encrypted-by-Default-08-14

WhatsApp account number at issue.[84] In contrast, WeChat's data retention policy permits the retention of personal information "for so long as is necessary to fulfil the purposes for which it was collected," including for responding to government requests and compliance with applicable laws and regulations.[85]

32. *Transparency and User Education*: Transparency and education about the level of security messaging apps provide are also integral to the responsibility to respect users' privacy. As part of their responsibility to conduct due diligence, the UN Guiding Principles require companies to communicate potential human rights impacts to affected users, other relevant stakeholders, and the general public.[86] Civil society, inter-governmental bodies, and multi-stakeholder groups have provided the ICT sector with detailed guidance on the information and analysis they should disclose about the privacy and freedom of expression implications of their products and services.[87]

33. For messaging apps that require users to enable end-to-end encryption and other additional layers of security, it is critical to provide users with clear and accessible information about how to enable these features and use them properly. They should also educate users on the degree of privacy and security protection offered by default settings. However, the accessibility of such information may differ based on the user's operating system. For example, on Facebook Messenger for iOS, the option to enable "secret," end-to-end encrypted chats is immediately apparent when a user starts a new conversation. In contrast, once Android users select the option to begin a new conversation, they must also select an information icon in the upper corner of their screen before they can access the "secret conversation" function. Although Facebook includes these steps in its Help Center, such information is not readily available in app.

To start a secret conversation:

iPhone or iPad:

1. From **Home**, tap in the top right.
2. Tap **Secret** in the top right.
3. Select who you want to message.
4. If you want, tap in the text box and set a timer to make the messages disappear.

Android:

1. From the tab, open a conversation with the person you want to have secret conversation with
2. Tap in the top right of the conversation.
3. Tap **Go to Secret conversation**.
4. If you want, tap in the text box and set a timer to make the messages disappear.

Secret conversations are currently only available in the Messenger app on iOS and Android, so they won't appear on Facebook chat or messenger.com.

---

[84] WhatsApp, *Information for Law Enforcement Authorities*, available at https://faq.whatsapp.com/en/android/26000050/?category=5245250

[85] WeChat, *WeChat – Privacy Policy* (last modified December 8, 2017), available at https://www.wechat.com/en/privacy_policy.html

[86] See United Nations, *Guiding Principles*, supra n. 50 at Principle 21.

[87] See A/HRC/35/22, *supra* n. 1; A/HRC/38/35, *supra* n. 1; Ranking Digital Rights, *Corporate Accountability Index*, available at https://rankingdigitalrights.org/index2017/; GNI, *Implementation Guidelines*, *supra* n. 70.

34. In contrast, initiating secret conversations on Telegram is equally intuitive on both iOS and Android, and the option to activate a "secret" chat is immediately visible once user s start a new chat:

Q: How do I start a secret chat?

iOS: Start a new message (tap the icon in the top-right corner in Messages). Then 'New secret chat'.
Android: Swipe right to open the menu, then 'New secret chat'.
WP: Tap + in the chats list, then 'New secret chat'.

Remember that Telegram secret chats are device-specific. If you start a secret chat with a friend on one of your devices, this chat will only be available on that device. If you log out, you will lose all your secret chats. You can create as many different secret chats with the same contact as you like.

35. Furthermore, Telegram and Viber provide informative and easy-to-understand responses to Frequently Asked Questions regarding differences between default and optional levels of security on their websites, but it is unclear whether such information is also accessible in app.[88] LINE also has a dedicated Encryption Status Report that provides an overview of the different levels of encryption available to users by message type (i.e. text, images, voice).[89] Several companies also provide technical "white papers" that explain the platform's encryption and security protocols in greater detail.[90]

B. Device Manufacturers

36. Although end-to-end encryption allows users to protect their information "in transit", users' communications and other sensitive data may nevertheless remain vulnerable to attack directly through laptops, mobile phones and hard drives. The Internet of Things has also broadened the range of Internet-connected devices and systems that collect, transmit and analyze personal and private information on a daily basis. These include home automation devices (such as Amazon Echo and Google Home), smart thermostats, home security systems, connected cars and baby monitors.91 Without appropriate encryption protocols and security measures, these devices could render users vulnerable to financial crimes (such as identity theft and fraud) and threats to their physical safety and well-being (such as device hacking leading to overheating in homes and car crashes).[92]

37. To ensure the security of vital personal information, device manufacturers have created built-in encryption tools to prevent unauthorized individuals from accessing users' devices. Although the technology differs by company and device, device encryption generally makes data stored on the device indecipherable without a key – typically as password/passcode – to unlock the device.

---

[88] Telegram, *Telegram FAQ*, available at https://telegram.org/faq#q-how-secure-is-telegram; Rakuten Viber Support, *Viber accounts security and encryption* (last updated April 15, 2018), available at https://support.viber.com/customer/en/portal/articles/2017401-viber-accounts-security-and-encryption#group-chats.

[89] LINE, *LINE Encryption Status Report* (September 13, 2017), available at https://linecorp.com/en/security/encryption_report

[90] For example, WhatsApp published a white paper that provides an in-depth technical explanation of the platform's encryption technology and use of the "Signal Protocol". WhatsApp, *WhatsApp – Encryption Overview Technical white paper*. available at https://www.whatsapp.com/security/WhatsApp-Security-Whitepaper.pdf. Similarly, LINE issued a 17-page technical white paper that "provides technical details about the encryption protocols and algorithms used in LINE's messaging and VoIP platform." Line, *Line Encryption Overview: Technical White Pape* (September 29, 2016), available at https://scdn.line-apps.com/stf/linecorp/en/csr/line-encryption-whitepaper-ver1.0.pdf.

[91] Consumers Union, "Beyond Secrets: The Consumer Stake in the Encryption Debate" (Dec 21, 2017), *available at* https://consumersunion.org/wp-content/uploads/2017/12/Beyond-Secrets-12.21.17-FINAL.pdf.

[92] *Id.*

38. Some personal computer and laptop manufacturers have begun encrypting their devices by default and in ways that are easy to use for individuals without significant technical knowledge. For example, Apple's FileVault disk encryption program became a default feature on all Macintosh computers in October 2014[93] and works by automatically encrypting data as it is downloaded on to the computer's start-up disk. Users are then able to unlock their device simply by entering their computer password[94]. User-friendly disk encryption programs like FileVault allow users to simply opt-in (or opt-out) of the program and automatically obtain a significant layer of security and privacy to protect their information without going through complicated technical steps. However, user intuitiveness may also raise security concerns, if for example, an unauthorized individual is able to obtain or guess your computer password.

39. Many mobile phone operating systems also incorporate forms of device security. Apple, which claims to have "designed the iOS platform with security at its core" uses a combination of hardware and software, including device encryption, to protect users' data.[95] In contrast, Google's Android operating system does not universally provide device encryption by default, but typically supports both full-disk and file-based encryption, giving the user greater autonomy over their device's security.[96] However, devices that run the Android operating system that are produced by certain manufacturers may be incapable of supporting device encryption.[97]

40. Finally, even in cases where companies adopt stringent security features, absolute device security may be impossible to achieve. As discussed earlier, the device encryption features in Apple' iOS prevented the U.S. FBI from gaining access to a suspect's iPhone following a 2015 shooting in San Bernardino. Nevertheless, the law enforcement agency was ultimately able to gain access to the suspect's device through the assistance of an outside contractor which "can determine or disable the PIN, pattern, password screen locks or passcodes on the latest Apple iOS and Google Android devices".[98] These forms of hacking pose serious threats to device security, even for devices operating at the highest levels of security. They also raise important questions about the human rights responsibilities of companies that provide these services to law enforcement and other government agencies.

C. Digital Access Providers

41. Private actors at the infrastructure layer of the Internet also play critical roles in protecting encryption. Internet Service Providers ("ISPs"), long at the forefront of the digital access industry, "operate and sell access to the series of networks that comprise the Internet."[99] While ISPs are generally not directly involved in encrypting Internet traffic and communications, they are nevertheless responsible for creating an operating environment that maintains and ensures the privacy and security of encrypted traffic transmitted through their networks.

---

[93] *Apple defies FBI and offers encryption by default on new operating system*, The Guardian (Oct. 17 2014), available at https://www.theguardian.com/technology/2014/oct/17/apple-defies-fbi-encryption-mac-osx

[94] Apple, *Use FileVault to encrypt the startup disk on your Mac* (Dec. 18, 2017), available at https://support.apple.com/en-us/HT204837

[95] Apple, *iOS Security* (January 2018), available at https://www.apple.com/business/docs/iOS_Security_Guide.pdf

[96] Android Source, *Security* (May 8, 2018), available at https://source.android.com/security/encryption/

[97] Microsoft, *Your Android device seems to be encrypted, but Company Portal says otherwise* (Nov. 14, 2017), available at https://docs.microsoft.com/en-us/intune-user-help/your-device-appears-encrypted-but-cp-says-otherwise-android

[98] Thomas Fox-Brewster, *The Feds Can Now (Probably) Unlock Every iPhone Model In Existence -- UPDATED*, Forbes (February 26, 2018) available at https://www.forbes.com/sites/thomasbrewster/2018/02/26/government-can-access-any-apple-iphone-cellebrite/#571d2ff9667a

[99] A/HRC/35/22, *supra* n. 4 at 30.

42. The importance of ISPs stems in part from their unique access to sensitive and revealing metadata about encrypted traffic. For example, although encrypted web traffic may prevent ISPs from accessing content and URL information, unsecured metadata will almost always reveal the domain names that their users visit.[100] Furthermore, ISPs enjoy unique access to information about the distinctive features of network traffic, such as the "size, timing and destination of the encrypted packets."[101] Over time, such information is capable of revealing the types of websites or pages visited, where and how frequently they were accessed, and even web search queries.[102] Such information may be used not only to facilitate government censorship and surveillance, but also for advertising purposes and to interfere with net neutrality. Although there is little or no information about whether companies in fact collect and analyze data about encrypted network traffic, researchers have previously discovered attempts by ISPs in the United States and Thailand to tamper with e-mail encryption.[103]

43. As gatekeepers of the Internet, the design and engineering choices that ISPs make about the development of their network architecture also assume human rights importance. The Special Rapporteur has urged ISPs and other digital access providers to "assume an active and engaged role in developing expression and privacy enhancing measures," and incorporate human rights safeguards by design wherever possible.[104] ISPs, for example, should evaluate their role in the development of innovative censorship circumvention technologies like refraction networking, which makes it more difficult for governments to block and monitor access to encryption tools and other websites and services.[105]

44. Many ISPs have affirmed their commitment to the privacy and security of their users. For example, AT&T assures its users that it has established "electronic and administrative safeguards designed to make the information we collect secure."[106] Telenor pledges to "always take steps to ensure that we keep your personal information safe and secure."[107] Vodafone maintains that "[r]espect for privacy is a key component in the design, development and delivery of our products and services."[108] Member ISPs of the Global Network Initiative, a multi-stakeholder initiative that seeks to hold ICT companies accountable to human rights standards, also commit to "employ[ing] protections with respect to personal information in all countries where they operate," particularly when confronted with government demands, laws or regulations that unduly compromise privacy.[109]

45. However, it is less clear how ISPs undertake human rights due diligence and other appropriate action to ensure respect for the privacy of encrypted communications and network traffic. For example, Vodafone, the top-ranked telecommunications company in the Ranking Digital Rights Index,[110] does not explicitly discuss whether and how it analyzes encrypted traffic and whether it seeks to infer its contents based on metadata and other secondary traits. Nevertheless, it explains that it examines "data packets" to "identify

---

[100] Upturn, "What ISPs Can See" (Mar. 2016), *available at* https://www.teamupturn.org/reports/2016/what-isps-can-see

[101] *Ibid.*

[102] *Ibid.*

[103] Electronic Frontier Foundation, "ISPs Removing Their Customers' Email Encryption" (11 November 2014), *available at* https://www.eff.org/deeplinks/2014/11/starttls-downgrade-attacks

[104] A/HRC/35/22, *supra* n. 1 at 59.

[105] Refraction Networking, https://refraction.network/.

[106] AT&T "Privacy Policy FAQ" (last visited 8 May, 2018), *available at* http://about.att.com/sites/privacy_policy/terms#collect

[107] Telenor Group, "Understanding Our Privacy Position" (last visited May 8, 2018), *available at* https://www.telenor.com/sustainability/responsible-business/privacy-and-data-protection/understanding-our-privacy-position/

[108] Vodafone, "Privacy Commitments" (last visited May 8, 2018), *available at* http://www.vodafone.com/content/index/about/privacy.html

[109] Global Network Initiative, "Principles on Freedom of Expression and Privacy" (May 2017), *available at* https://globalnetworkinitiative.org/gni-principles/

[110] Ranking Digital Rights, "Key Findings: Vodafone Group, Plc" (Jan 12, 2018), *available at* https://rankingdigitalrights.org/index2018/companies/vodafone/

the type of communication" for network traffic management purposes.[111] The "use of network technologies that inspect data packets" for other purposes requires an "in-depth privacy impact assessment," but the specific uses of such technologies and the criteria and outcomes of such assessments have not been disclosed.[112]

46. AT&T, another large, multi-national telecommunications company, is also silent on how it handles encrypted traffic but admits that it collects a constellation of information about "how you use our networks" to learn about "the pages you visit, the time you spend, the links or advertisements you see and follow, [and] the search terms you enter."[113] The company provides even less detail than Vodafone about how it secures such information, publishing only a general list of "electronic and administrative safeguards."[114] It also retains such information "as long as we need it for business, tax or legal purposes."[115]

47. Content Delivery Networks ("CDNs"), which provide web hosting and other online services that facilitate digital access, have also come under intense scrutiny for their role in disabling access to encryption and censorship circumvention tools.[116] In countries where these tools are blocked, providing access relies on a network manipulation technique known as 'domain fronting,' which disguises web traffic to and from the blocked service as traffic to an entirely different website, usually hosted on major CDNs such as Google Cloud CDN, Amazon CloudFront and Cloudflare. In April 2018, Russia's ban on Telegram extended to a large number of Amazon and Google IP addresses, in a bid to prevent users from circumventing the ban through domain fronting.[117] Also this spring, Google and Amazon announced changes to their cloud services infrastructure that effectively blocked domain fronting.[118] Digital rights advocates have criticized the companies' moves for their adverse impact on privacy and freedom of expression in repressive regimes, where these tools are critical to secure communications among human rights defenders, activists and other communities-at-risk.[119]

IV. Recommendations

A. Recommendations to States:

48. States should adopt laws and policies that provide comprehensive protection for and support the use of encryption tools, including encryption tools designed to protect anonymity ("encryption and anonymity tools"). Legislation protecting human rights

---

[111] Vodafone, "Privacy and Security: Managing Privacy and Security Risks" (June 2015), *available at* http://www.vodafone.com/content/sustainabilityreport/2015/index/operating-responsibly/privacy-and-security.html

[112] *Ibid.*

[113] Telenor Group, "How We Collect Personal Information About You" (last visited May 8, 2018), *available at* https://www.telenor.com/sustainability/responsible-business/privacy-and-data-protection/understanding-our-privacy-position/#how-we-collect-personal-information-about-you

[114] AT&T, *supra* n. 106.

[115] *Ibid.*

[116] For a more detailed explanation of the functions and human rights value of CDNs, see A/HRC/35/22, *supra* n. 1 at 36.

[117] British Broadcasting Corporation, Russia Telegram ban hits Google and Amazon services (Apr 23, 2018), *available at* https://www.bbc.com/news/technology-43865538.

[118] Thomas Claburn, *Google kills off domain fronting – and so secure comms just got tougher*, The Register (Apr 19, 2018), *available at* https://www.theregister.co.uk/2018/04/19/google_domain_fronting/; Signal, Amazon threatens to suspend Signal's AWS account over censorship circumvention (May 1, 2018), *available at* https://signal.org/blog/looking-back-on-the-front/.

[119] Access Now, "Message to Google and Amazon on domain fronting: You break it, you bought it" (2 May 2018), *available at* https://www.accessnow.org/message-to-google-and-amazon-on-domain-fronting-you-break-it-you-bought-it/; Tom Spring, *Free Speech Advocates Blast Amazon Over Threats Against Signal*, Threatpost (3 May 2018), *available at* https://threatpost.com/free-speech-advocates-blast-amazon-over-threats-against-signal/131640/.

defenders, journalists, artists, academics and civil society should also be enacted and include support for the use of such tools.

49. Laws should be established or amended to specify clearly that restrictions on encryption and anonymity tools, including government hacking measures, are permitted only in exceptional circumstances; *i.e.* when they satisfy the requirements of legality, necessity and proportionality, and legitimacy of objective. Government authorities should refrain from relying on generic or antiquated laws to justify restrictions on encryption and anonymity tools that do not satisfy these criteria.

50. Laws that ban encryption and anonymity tools or require their registration before their use or dissemination do not meet the criteria of legality, necessity and proportionality. Additionally, States should not require private actors to facilitate backdoor access in commercially available products and services. States should also refrain from laws that mandate local storage of *all* user data (including encryption keys) or the establishment of key escrows.

51. When proposing restrictions on encryption and anonymity tools, States should engage in a meaningful and transparent consultations with a representative cross-section of civil society, corporations, the general public, and relevant stakeholders concerning the appropriate scope of those restrictions.

52. Laws that provide for court-ordered decryption or hacking should require the authorization, on a case-by-case basis, of an independent and impartial judicial body of the proposed decryption or hacking order. The judicial body should review the order to ensure that it meets the requirements of legality, necessity, proportionality and legitimacy of objective.

B. Recommendations to Companies:

53. Given the importance of encryption to digital communication, access to information and other essential activities, companies, both in and outside the ICT sector, should evaluate the extent to which the business activities implicate the digital security and privacy of individuals. Such impact assessments should be part of the company's responsibility to conduct human rights due diligence and lead to both high-level policy commitments and internal policies and processes that ensure respect for digital privacy and related human rights throughout its operations.

54. Companies that offer messaging apps and device manufacturers should evaluate their responsibility to provide encryption features in their products and services. Assessments on how best to design and update these features in light of security, usability, feasibility, costs and other relevant considerations should be conducted on an ongoing basis and ensure meaningful input from customers and other affected rights holders, civil society, technologists with human rights background, and the broader human rights community. As a general rule, companies should seek to provide the highest user privacy settings by default. If this is not possible, they should ensure that "opt-in" settings are highly visible and user-friendly and provide clear and accessible information about the differences between various privacy settings.

55. Digital access providers should conduct human rights due diligence and take other appropriate action to ensure respect for the privacy and security of end users. They should provide meaningful and accessible guidance on how they analyze, use and retain information about encrypted traffic in their company policies and transparency reporting, including any technical and policy safeguards to prevent undue government or private interference with such traffic.